CLAIMS

1. A defense device that controls, based on information on an attack against a server or a domain, a passage of a malicious packet addressed to the server or the domain on a network by transmitting route information to a repeater that relays the malicious packet, the defense device comprising:

a repeater selecting unit that selects at least one repeater that becomes a notification destination of the route information for routing the malicious packet through the defense device, from among a plurality of repeaters adjacent to the defense device, based on the information on the attack;

a route-information notifying unit that notifies the route information for routing the malicious packet through the defense device to the repeater by the repeater selecting unit; and

a packet control unit that controls the passage of the malicious packet routed to the defense device from the repeater to which the route information has been notified by the route-information notifying unit.

2. The defense device according to claim 1, wherein

the repeater selecting unit selects the repeater as the notification destination of the route information, excluding the repeater that becomes a next relay destination with respect to the server or the domain attacked by the malicious packet, from among the repeaters adjacent to the defense device.

3. The defense device according to claim 1 or 2, further comprising:

an attack information transmitter that transmits the

information on the attack to other defense device adjacent to the defense device, wherein

the repeater selecting unit also selects, when the information on the attack is received from the other defense device, at least one repeater that becomes the notification destination of the route information for routing the malicious packet through the defense device, based on the information on the attack.

4. The defense device according to claim 1, further comprising:

an attack-termination determining unit that monitors the malicious packet routed to the defense device from the repeater to which the route information has been notified by the route-information notifying unit, and determines whether a transmission of the malicious packet routed from the repeater to the defense device has terminated, wherein

when the attack-termination determining unit determines that the transmission of the malicious packet has terminated, the route-information notifying unit notifies route information for not routing the malicious packet through the defense device to the repeater.

5. A network-attack defense system comprising:

a plurality of repeaters that relays a packet transmitted to a server or a domain on a network; and

a defense device that controls, based on information on an attack against the server or the domain, a passage of a malicious packet addressed to the server or the domain on a network by transmitting route information to a repeater that relays the malicious packet, wherein

the defense device includes

a repeater selecting unit that selects at least

one repeater that becomes a notification destination of the route information for routing the malicious packet through the defense device, from among a plurality of repeaters adjacent to the defense device, based on the information on the attack;

a route-information notifying unit that notifies the route information for routing the malicious packet through the defense device to the repeater by the repeater selecting unit; and

a packet control unit that controls the passage of the malicious packet routed to the defense device from the repeater to which the route information has been notified by the route-information notifying unit.

6. A defense method using a defense device that controls, based on information on an attack against a server or a domain, a passage of a malicious packet addressed to the server or the domain on a network by transmitting route information to a repeater that relays the malicious packet, the defense method comprising:

selecting at least one repeater that becomes a notification destination of the route information for routing the malicious packet through the defense device, from among a plurality of repeaters adjacent to the defense device, based on the information on the attack;

notifying the route information for routing the malicious packet through the defense device to the repeater at the selecting; and

controlling the passage of the malicious packet routed to the defense device from the repeater to which the route information has been notified at the notifying.

7. The defense method according to claim 6, wherein

the selecting includes selecting the repeater as the notification destination of the route information, excluding the repeater that becomes a next relay destination with respect to the server or the domain attacked by the malicious packet, from among the repeaters adjacent to the defense device.

8. The defense method according to claim 6 or 7, further comprising:

transmitting the information on the attack to other defense device adjacent to the defense device, wherein

the selecting includes also selecting, when the information on the attack is received from the other defense device, at least one repeater that becomes the notification destination of the route information for routing the malicious packet through the defense device, based on the information on the attack.

9. The defense method according to claim 6, further comprising:

monitoring the malicious packet routed to the defense device from the repeater to which the route information has been notified at the notifying; and

determining whether a transmission of the malicious packet routed from the repeater to the defense device has terminated, wherein

when it is determined that the transmission of the malicious packet has terminated, the notifying includes notifying route information for not routing the malicious packet through the defense device to the repeater.

10. A defense program for realizing a defense method using a defense device that controls, based on information on an

attack against a server or a domain, a passage of a malicious packet addressed to the server or the domain on a network by transmitting route information to a repeater that relays the malicious packet, the defense program causing a computer to execute as the defense device:

selecting at least one repeater that becomes a notification destination of the route information for routing the malicious packet through the defense device, from among a plurality of repeaters adjacent to the defense device, based on the information on the attack;

notifying the route information for routing the malicious packet through the defense device to the repeater at the selecting; and

controlling the passage of the malicious packet routed to the defense device from the repeater to which the route information has been notified at the notifying.

11. The defense program according to claim 10, wherein

the selecting includes selecting the repeater as the notification destination of the route information, excluding the repeater that becomes a next relay destination with respect to the server or the domain attacked by the malicious packet, from among the repeaters adjacent to the defense device.

12. The defense program according to claim 10 or 11, further causing the computer to execute:

transmitting the information on the attack to other defense device adjacent to the defense device, wherein

the selecting includes also selecting, when the information on the attack is received from the other defense device, at least one repeater that becomes the notification destination of the route information for

routing the malicious packet through the defense device, based on the information on the attack.

13. The defense program according to claim 10, further causing the computer to execute:

monitoring the malicious packet routed to the defense device from the repeater to which the route information has been notified at the notifying; and

determining whether a transmission of the malicious packet routed from the repeater to the defense device has terminated, wherein

when it is determined that the transmission of the malicious packet has terminated, the notifying includes notifying route information for not routing the malicious packet through the defense device to the repeater.